RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCEMAGAZINE

SPECIAL ISSUE

IT SECURITY

Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications

#33 Volume

Special Issue 2023

The calculations for the RAC-COON attack were run on the Chair's own cloud.

THE TELLTALE

Attacks on the TLS protocol are both rare and highly complex. And yet, the encryption experts at Ruhr University Bochum are constantly tracking down new ones.

The thick volume that contains all technical details on the TLS encryption protocol has roughly a thousand pages. This means that the TLS standard is as thick as three Harry Potter novels. "It takes a lot of time and crypto know-how to understand and keep track of all of its features," says Dr. Robert Merget from the Chair for Network and Data Security at the Horst Görtz Institute for IT Security at Ruhr University Bochum, which has been specialising in Transport Layer Security (TLS) for years. This cryptographic encryption protocol ensures that, for example, connections between internet browsers and servers or between different email servers are secure. Merget and his colleagues know the standard pretty much by heart and have consequently mastered every trick and every TLS encryption spell.

They have been developing a TLS analysis tool since 2015. It enables companies to implement TLS with as few errors as possible to ensure that there are no security gaps left for attackers to exploit. Almost every day, the researchers come across vulnerabilities that occur during implementation, so-called bugs. "By contrast, systematic attacks on the TLS standard have become rather rare," points out Merget. But they do still happen. In 2020, the encryption expert discovered a highly specialised attack on a specific TLS algorithm, and alerted the crypto community to the threat of a malicious RACCOON attack.

"We use easy-to-remember names for vulnerabilities that are otherwise quite technical. This makes it easier for us to talk about them in the community," explains Merget. While research institutes are part of the community, it is primarily IT companies such as Google, Microsoft and Cloudflare who have a vested interest in ensuring that TLS is as secure as possible and who are constantly trying to improve it.

The TLS encryption protocol is public and can be viewed by all. "The algorithms are public, but the keys that are used are secret," outlines Merget. "Think of it like a secret ▸

language." When using a secret language in the past, it was often done by swapping letters. People who knew the exact code – that is, who knew which letter had to be substituted for another letter – were able to decode the message. However, keeping the method a secret turned out to be quite difficult and insecure. This is why today's encryption experts choose a different approach. "Modern algorithms are public, but the keys for the algorithms are secret. It's the same with TLS. The attacker has access to the encryption principle, but the keys are kept secret," explains Merget. The main purpose of TLS cryptography is to prevent third parties from intercepting communications. Moreover, the protocol has two additional properties: firstly, TLS is used for authentication, and secondly for data integrity.

About four billion users worldwide use TLS today. And each of them has different preferences and requirements for the encryption protocol. This explains why so many developers have been refining and tweaking the TLS standard for years – and also why the protocol is today considered secure. This was, after all, not always the case. "Since 1994, since TLS has been created, the protocol has been the target of numerous attacks. Most notably, there were many attacks between 2011 and 2016," says Merget. But as he points out: "As a rule, this is not an attack that can be carried out by your local neighbourhood hacker. These are difficult high-tech attacks, such as might be executed by secret services. Usually, ordinary users have nothing to fear from them." Since 2018, since the introduction of the modernised TLS 1.3 standard, the number of attacks has decreased significantly. And yet: attacks on the TLS versions introduced between 1996 and 2018 do still take place. In 2020, Robert Merget discovered the vulnerability in question, which he dubbed RACCOON.

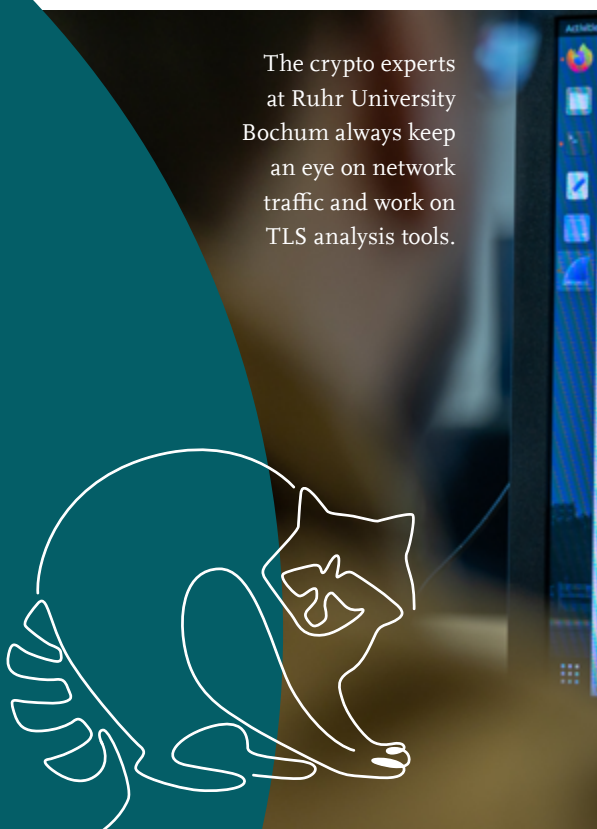
The RACCOON attack targets the so-called Diffie-Hellman key exchange protocol, i.e. a very specific algorithm that can be used in TLS to ensure that, for example, a bank and its client can exchange a shared secret, a shared key. In very concrete terms, the attacker exploits a timing vulnerability in the key derivation when the Diffie-Hellman algorithm is used:

i THE INVENTION OF TLS

The encryption protocol TLS was developed in 1994 by the company Netscape (today: Firefox) and was initially called SSL (the acronym stands for: Secure Sockets Layer). In 1999, the Internet Engineering Task Force renamed SSL in TLS, because they believed that the protocol for data security on the internet shouldn't be in the hands of one corporation.

The focus of Robert Merget's research is on the TLS encryption protocol

> "SINCE 1994, SINCE TLS HAS BEEN CREATED, THE PROTOCOL HAS BEEN THE TARGET OF NUMEROUS ATTACKS."
>
> Robert Merget



The crypto experts at Ruhr University Bochum always keep an eye on network traffic and work on TLS analysis tools.

the duration of the key derivation and with it the cryptographic processing of the secret gives the attacker the information he needs to decrypt the data and, as a result, to break the confidentiality of the protocol.

"Timing is a so-called side channel, one of many, that allows us to infer the secret key of an algorithm and possibly even to crack it," elaborates Merget. "Let's say I encrypt the word dog or the word mouse. It takes longer for me to encrypt the word mouse because it has more letters. An attacker can measure the time it takes me to encrypt communication, and then use the measured time to deduce what was encrypted." In addition to time, factors such as rising temperatures or the power consumption of devices likewise provide information about the computing operations of an algorithm – these, too, are side channels that may enable attackers to obtain keys.

The concept behind the RACCOON attack is easy to understand. "Broadly speaking, the Diffie-Hellman key is always based on calculations with a remainder," says Merget. In the mathematical derivations of the Diffie-Hellman key exchange, calculations are continued with the remainder without the leading zeros.

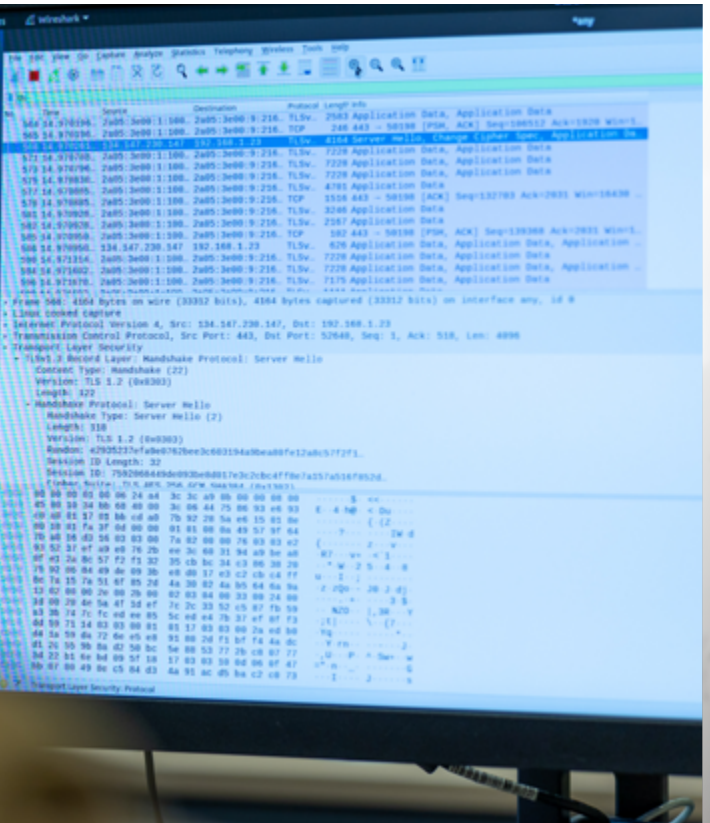
"Processing smaller numbers can be done more rapidly because of the smaller data volume. This gives the attacker an advantage: he observes how fast an operation was executed and then concludes whether or not there was a leading zero," explains Merget. This is the vulnerability that the attacker exploits. He can then reconstruct the secret key from the information he has gathered. "However, to do this, he needs complicated mathematical procedures used in linear algebra," adds Merget.

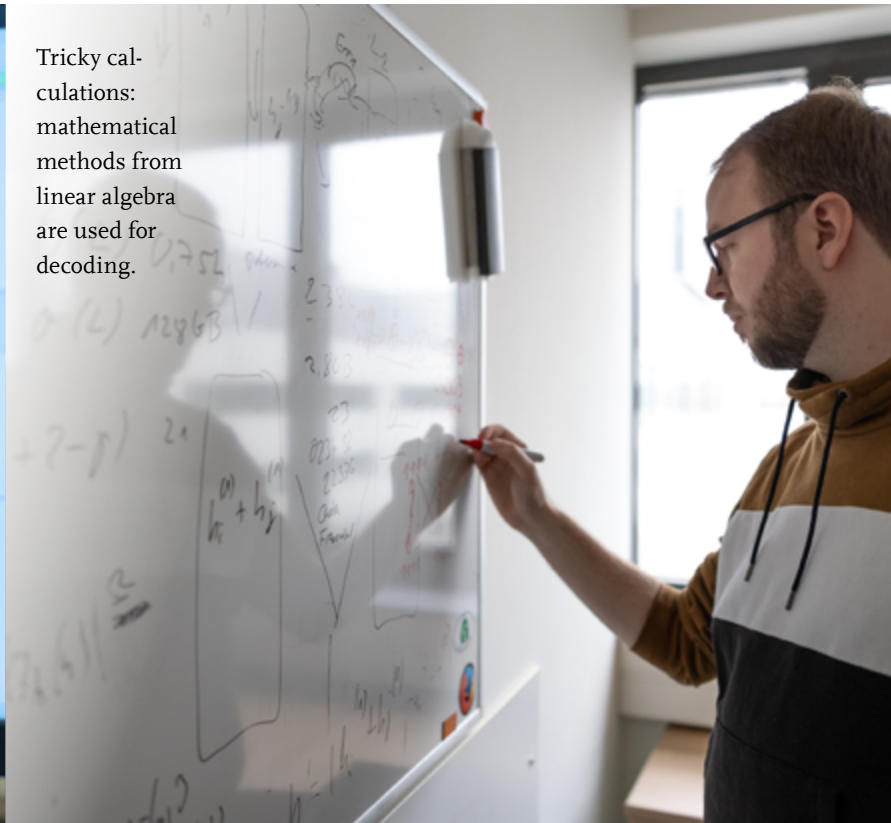
To find out just how widespread the vulnerability is, Merget sent data packets via a dedicated internet line to approximately 100,000 servers that use TLS. "Three per cent of the world's internet responded and was affected by this vulnerable TLS configuration," points out Merget.

"In the first step, we contacted all developers of major TLS implementations and warned them. We then reported the case to the Federal Office for Information Security and asked them to support us in the so-called responsible disclosure process," says Merget. The purpose of this process for the disclosure of security vulnerabilities, which is well-established in IT security, is to notify manufacturers promptly about vulnerabilities and to provide updates and patches before the public becomes aware of them.

But how can the vulnerability be fixed? "The best course of action is to use the latest and most secure version of TLS, TLS 1.3," recommends Merget. Overall, however, the researcher is convinced that the TLS protocol is very secure: "It is extremely difficult to still detect vulnerabilities."

text: lb, photos: ms





Tricky calculations: mathematical methods from linear algebra are used for decoding.

EDITOR'S DEADLINE

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

↗ *casa.rub.de/en/outreach/science-comics*

Answers
DEEP FAKE-QUIZ
The following faces are real:
1a, 2a, 3b, 4a, 5b, 6a

LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

GRAPHIC DESIGN, ILLUSTRATION, LAYOUT:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639